



**Homeland
Security**

Daily Open Source Infrastructure Report

30 March 2012

Top Stories

- The former superintendent of a southern West Virginia mine where an explosion killed 29 workers pleaded guilty March 29 to a federal fraud charge. Prosecutors said he manipulated the mine ventilation system during inspections, and he disabled a methane monitor a few months before the fatal explosion. – *Associated Press* (See item [1](#))
- A special agent in charge of Homeland Security investigations warned counterfeit airbags were being sold in the Detroit market and could cause injuries in the event of deployment. – *WDIV 4 Detroit* (See item [9](#))
- The head of the National Security Agency and Cyber Command told a U.S. Senate panel that China stole a great deal of the U.S. military's intellectual property from defense contractors. – *CNET News* (See item [10](#))
- Four U.S. Navy employees and three defense contractors pleaded guilty to a scheme that involved awarding millions of dollars in aircraft maintenance contracts in exchange for bribes. – *Associated Press* (See item [11](#))
- Firefighters rescued two people who passed through an unlocked gate and scaled several fences to break into a pump house at a water treatment plant in Sacramento, California. – *KOVR 13 Sacramento* (See item [33](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Agriculture and Food](#)
- [Water](#)
- [Public Health and Healthcare](#)

SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
- [Emergency Services](#)
- [National Monuments and Icons](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: LOW, Cyber: LOW

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - <http://www.esisac.com>]

1. *March 29, Associated Press* – (West Virginia) **Ex-super pleads guilty in W.Va. mine blast case.** The former superintendent of a southern West Virginia mine where an explosion killed 29 workers pleaded guilty March 29 to a federal fraud charge. The highest-ranking Massey Energy official charged in connection with the blast faces up to 5 years in prison when sentenced August 9. Prosecutors said the man manipulated the mine ventilation system during inspections to fool safety officials, and disabled a methane monitor on a cutting machine a few months before the explosion April 5, 2010. It was not clear from court papers whether the device was ever fixed. Prosecutors accused Massey of violating many safety laws out of a desire to put production and profits first. Three investigations concluded the firm allowed highly explosive methane and coal dust to build up inside the mine, where it was ignited by a spark from an improperly maintained piece of cutting equipment. Clogged and broken water sprayers then allowed what could have been just a flare-up to become an epic blast, the investigations found.

Source: <http://www.miamiherald.com/2012/03/29/2720734/ex-super-pleads-guilty-in-wva.html#more>

2. *March 29, Associated Press* – (Maine) **3 indicted in theft of copper from Maine utility.** A former employee of Bangor Hydro-Electric Co. and two others were indicted on charges of stealing copper wire worth \$35,000 from the utility. A grand jury in Penobscot County, Maine, indicted the three men March 28. Prosecutors said one man was employed by Bangor Hydro when the theft occurred and another owned a scrap metal business. The suspects face up to 5 years in prison if convicted. The wire was taken within the past year from storage and was not in use when it was stolen.

Source:

<http://www.thenorthwestern.com/usatoday/article/38914623?odyssey=mod|newswell|text|FRONTPAGE|s>

3. *March 29, KARE 11 Minneapolis* – (Minnesota) **Highway 52 re-opens after semi rollover in Goodhue Co.** Highway 52 in Goodhue County, Minnesota, reopened after being closed in both directions for 7 hours March 29 due to a truck rollover that caused a gasoline spill, according to the Minnesota Department of Transportation. The rollover happened between Highway 57 and County Road 9. The state patrol said the semi carrying 8,800 gallons of gasoline went off the road into the median. The driver of the semi was ejected and air lifted hospital with non-life-threatening injuries. Authorities said there was a minor fuel leak.

Source: <http://www.kare11.com/news/article/970143/396/Highway-52-closed-in-both-directions-in-Goodhue-Co>

4. *March 28, Associated Press* – (New Mexico) **10.2M settlement reached in NM coal waste lawsuit.** A 2-year legal battle over the disposal of millions of tons of coal combustion waste in northwestern New Mexico is on the verge of being settled with a \$10.2 million agreement announced March 28 by the Sierra Club, a BHP Billiton mining company, and the state's largest electric utility. Settlement documents were filed by the groups in court in Albuquerque. The agreement is awaiting approval from a federal judge. The settlement calls for \$8 million to be spent on structures to prevent contaminants from reaching the San Juan River as well as other environmental remediation projects. More than \$2 million would cover the Sierra Club's attorney and expert fees. The Sierra Club sued in 2010 to stop the disposal in unlined pits of waste left over from burning coal at the San Juan Generating Station, a 1,800-megawatt plant that provides electricity to 2 million customers in the Southwest. The group claimed toxins from coal combustion waste were leaching into ground and surface water. Under the settlement, the current system for capturing shallow groundwater would be expanded to include areas downstream from the power plant and the mine. The captured water would then be diverted to an evaporation pond.

Source:

<http://www.thenorthwestern.com/usatoday/article/38910937?odyssey=mod|newswell|text|FRONTPAGE|s>

For another story, see item [5](#)

[\[Return to top\]](#)

Chemical Industry Sector

5. *March 28, Associated Press* – (Virginia) **Toxic chemical releases decline 4.2 pct. in Va.** A new state report said toxic chemical releases from industries and federal facilities are declining in Virginia. An annual inventory released March 28 by the Virginia Department of Environmental Quality said toxic chemical releases into the air, land, and water totaled 46.3 million pounds in 2010, the latest available data. That is a 4.2 percent decrease from 2009. Toxic chemicals released into the air fell 5.8 percent, while water releases dropped 2.7 percent. Industries reported a total 911.4 million

pounds of toxic chemicals managed on-site, transferred off-site, or released on-site. That is up 1.1 percent from 2009. About 79 percent of all on-site releases were by chemical manufacturing, utilities, and food manufacturing industries.

Source: <http://www.businessweek.com/ap/2012-03/D9TPKT5O1.htm>

6. ***March 27, MLive.com* – (Michigan) Dow Chemical work plan for Midland soil cleanup outlines site history, land use.** One-quarter of the property Dow Chemical Co. will provide dioxin cleanup at in Midland, Michigan, is non-residential land, MLive.com reported March 27. The company's 78-page report outlines the site history, research summaries, and overall cleanup plan for the Midland Area Soils Corrective Action. Dow, with oversight from the Michigan Department of Environmental Quality, will test about 1,330 Midland homes, 40 residential-like properties, and 380 non-residential properties. Dow will provide cleanup for any homes with dioxin levels higher than 250 parts per trillion. Of the total 1,700 acres in the area, about 425 acres is residential land use, the report said. Residential land includes homes and residential-like properties, or day cares, nursing homes, children's schools, parks with grassy areas, playgrounds, and campgrounds. Non-residential land is universities and colleges without residence halls, businesses, sports arenas, places of worship, paved public spaces, fire stations, and day shelters. The report said historic waste burning and waste incineration are the primary source of elevated dioxins and furans found in surface soil. Dow filters emissions from its coal plants now, and monitoring shows the dust control program is effective, the company said.

Source:

http://www.mlive.com/midland/index.ssf/2012/03/dow_chemical_work_plan_for_midland_area_soils_outlines_history_city_land_use.html

For more stories, see items [22](#) and [28](#)

[\[Return to top\]](#)

Nuclear Reactors, Materials and Waste Sector

7. ***March 29, Newburyport Daily News* – (New Hampshire) Report finds breaches at plant.** A report released March 27 by the Nuclear Regulatory Commission (NRC) stated that while the Seabrook Station nuclear power plant in Seabrook, New Hampshire, is safe it committed two “very low significance violations” in its evaluation of its decaying concrete problem. The inspectors determined the concrete areas of an underground tunnel affected by the deterioration were “operable but degraded,” according to a NRC spokesman. The NRC believes the structural integrity of the affected walls was not an immediate concern, due to the safety margins inherent in their design and construction.

Source: <http://www.newburyportnews.com/local/x1437242208/Report-finds-breaches-at-plant>

[\[Return to top\]](#)

Critical Manufacturing Sector

8. *March 28, U.S. Department of Justice* – (Wisconsin) **Shipbuilder and ship engine manufacturer to pay for Clean Air Act violations.** Coltec Industries Inc. and National Steel and Shipbuilding Company (NASSCO) agreed to pay a civil penalty of \$280,000 and spend about \$500,000 on an environmental project to resolve alleged violations of the Clean Air Act (CAA) and the U.S. Environmental Protection Agency's (EPA) marine diesel engine air rules, the U.S. Department of Justice and the EPA announced March 28. The project will significantly reduce nitrogen oxide emissions from a testing stack at Coltec's Beloit, Wisconsin, engine-manufacturing facility, improving air quality for residents. Coltec and NASSCO also agreed to attach the required EPA engine labels to 40 ship engines that were previously unlabeled or improperly labeled.

Source: <http://www.maritime-executive.com/article/shipbuilder-and-ship-engine-manufacturer-to-pay-for-clean-air-act-violations>

9. *March 28, WDIV 4 Detroit* – (Michigan) **Homeland Security warns counterfeit airbags being sold in Metro Detroit.** A special agent in charge of Homeland Security investigations in Michigan and Ohio warned that counterfeit airbags are being sold in the Detroit market and could cause injuries in the event of deployment. “The bag literally explodes, sending shrapnel and dangerous items into the passenger,” he said. Many of the faulty airbags can be bought online for a few hundred dollars, while a real airbag is priced closer to \$1,000. The counterfeits either do not deflate when they need to, or they deflate or inflate with such force that the parts become projectiles.

Source: <http://www.clickondetroit.com/news/investigations/Homeland-Security-warns-counterfeit-airbags-being-sold-in-Metro-Detroit/-/1719314/9742934/-/a5s3wdz/-/>

[\[Return to top\]](#)

Defense Industrial Base Sector

10. *March 28, CNET News* – (International) **China nabbing ‘great deal’ of U.S. military secrets.** Testifying before the U.S. Senate Armed Services Committee March 27, the head of the National Security Agency (NSA) and Cyber Command said China is stealing a “great deal” of the U.S. military’s intellectual property, adding that the NSA sees “thefts from defense industrial base companies.” He confirmed speculation that China was behind 2011’s attacks on RSA. Those attacks proved extremely troublesome for U.S. defense contractors. In 2011, Chinese hackers allegedly stole data related to RSA’s SecurID two-factor authentication devices. Soon after, that information was used to break through security safeguards at defense contractors Lockheed Martin, L-3 Communications, and Northrop Grumman.

Source: http://news.cnet.com/8301-13506_3-57405684-17/china-nabbing-great-deal-of-u.s-military-secrets/

11. *March 28, Associated Press* – (California) **Navy employees, contractors plead guilty to fraud involving \$1 million in bribes in Calif.** Four U.S. Navy employees and three defense contractors working near San Diego pleaded guilty to participating in a wide-

ranging corruption scheme in which the contractors won millions of dollars in military orders after offering officials massage chairs, bicycles, flat screen TVs, and other bribes, federal officials announced March 28. The civilian employees who worked for a Navy aircraft maintenance program accepted a total of more than \$1 million in bribes, a U.S. attorney said. It was unclear if the scheme put national security or military operations at risk. An assistant U. S. attorney said the Navy employees worked for a program tasked with ensuring aircraft were combat ready at the Naval Air Station North Island in Coronado, near San Diego. The four Navy employees worked for the Navy's Fleet Readiness Center and were assigned to maintaining the Navy's Grumman E-2 Hawkeye, an early warning aircraft, and the C-2 Greyhound, a derivative of the E-2 that has a widened fuselage with a rear loading ramp. Officials said the Defense Department paid more than \$5.5 million in connection with fraudulent invoices submitted by the three defense contractors.

Source: http://www.washingtonpost.com/national/navy-officials-contractors-plead-guilty-to-fraud-involving-1-million-in-bribes-in-calif/2012/03/28/gIQAfcQwgS_story.html

[[Return to top](#)]

Banking and Finance Sector

12. *March 29, Empire State News* – (New York) **Stolen credit card information use to purchase \$100,000 worth of E-ZPass tags.** Charges were filed March 28 in New York against two defendants for engaging in a \$6 million Internet-based credit card fraud scheme. As part of their scheme, the defendants used stolen credit cards to purchase \$100,000 worth of E-ZPass tags and credits, which they then re-sold. They also caused fraudulent charges to be made on stolen credit and debit cards and created a bogus Web site that lured customers into purchasing products that they never received. In total, the pair compromised more than 1,400 credit and debit cards, attempting to charge more than \$6 million to these accounts. Both suspects were arrested March 28 at their home in Brooklyn.

Source: <http://www.empirestatenews.net/News/20120329-7.html>

13. *March 29, Forest Hills Patch* – (New York) **Alleged Queens Blvd. bandit arrested.** Police in the Queens borough of New York City have announced the arrest of a suspect wanted in connection with five bank robberies, three of which happened on Queens Boulevard, the Forest Hills Patch reported March 29. The suspect was arrested and charged with five counts of robbery for his alleged role in a February crime spree that struck four Chase Bank branches and one Capital One Bank. Police have been seeking a suspect since the first incident February 3. Every incident was similar, with the suspect handing a note to the teller then fleeing, with or without cash.

Source: <http://foresthills.patch.com/articles/alleged-queens-blvd-bandit-arrested>

14. *March 28, U.S. Department of the Treasury* – (International) **Treasury announces additional sanctions against Iranian engineering and shipping firms.** The U.S. Department of the Treasury announced March 28 additional sanctions against two entities connected to the network of the Islamic Revolutionary Guard Corps (IRGC)

and two individuals and two entities affiliated with Iran's national maritime carrier, the Islamic Republic of Iran Shipping Lines (IRISL). Pursuant to Executive Order 13382 Treasury designated several entities. The order is aimed at freezing the assets of proliferators of weapons of mass destruction and their supporters and thereby isolating them from U.S. financial and commercial systems. Entities designated by Treasury include: Iran Maritime Industrial Company SADRA (SADRA), an entity owned by the IRGC; Deep Offshore Technology PJS, a subsidiary of SADRA; Malship Shipping Agency Ltd., an IRISL affiliate; and Modality Limited, an IRISL affiliate.

Source: <http://www.treasury.gov/press-center/press-releases/Pages/tg1509.aspx>

15. *March 28, West Hawaii Today* – (Hawaii) **HCFCU admits member information breached.** Hawaii Community Federal Credit Union employees improperly accessed the names, addresses, and last four digits of Social Security numbers (SSNs) of “several hundred” Hawaii Community Federal Credit Union members, the credit union’s president said March 27. The data breach happened nearly a year ago. The credit union did not notify members until the week of March 26, while an attorney conducted an investigation, the president said. The credit union posted a letter on its Web site March 23, and mailed it to credit union members late the week of March 19, informing them of the data breach, which the president said happened in April 2011. The credit union has about 40,000 members. Fewer than 500 had their account information accessed, the president said. He said account information and full SSNs were not accessed. A credit union member filed a complaint in 2011 after becoming suspicious. The president said a “handful” of employees were involved in the breach. Disciplinary actions were “up to and including termination,” he added. Information from the investigation has been forwarded to federal authorities, he said. Credit union employees will go through new training to reinforce policies that bar accessing member data. Officials are also reviewing policies and procedures, the president said. Credit union employees will also be able to anonymously report suspicions they have about co-workers who may be improperly accessing information via a new Web site, he added.

Source: <http://www.westhawaiitoday.com/sections/news/local-news/hcfcu-admits-member-information-breached.html>

16. *March 28, U.S. Department of Justice* – (National) **Justice Department sues national tax preparation firm and franchisees to stop alleged pervasive tax fraud.** The United States has filed civil injunction lawsuits in five cities seeking to shut down both the company that operates Instant Tax Service (ITS) as well as five owners of ITS franchises, the Justice Department (DOJ) announced March 28. The government’s complaint accuses ITS Financial and its owner of deliberately ignoring systemic and pervasive fraud by ITS franchisees. The complaints allege franchisees across the country intentionally prepare and file fraudulent tax returns to maximize refunds. They do this so ITS Financial and its franchisees can extract large tax preparation fees and charges. The government claims the fees are outrageously high and are often not disclosed. The franchisees named in the complaints allegedly invent phony businesses, fabricate deductions, falsify filing statuses, claim bogus dependents, and disregard rules for claiming the earned income tax credit. The DOJ alleges ITS employees at these franchises have little tax preparation experience, and that the franchise owners encourage them to prepare fraudulent tax returns. The complaint against ITS Financial

states that the estimated tax losses from allegedly fraudulent return preparation in 2011 at ITS locations in St. Louis, the Kansas City area, Chicago, Indianapolis, and Las Vegas exceed \$16 million.

Source: <http://www.justice.gov/tax/2012/txdv12393.htm>

17. *March 28, U.S. Department of Justice* – (Texas) **Justice Department seeks to shut down Texas tax return preparer.** The United States has sued a tax preparer, seeking to bar him from preparing any federal tax returns for others, the Justice Department announced March 28. The civil injunction suit alleges the DeSoto, Texas man claimed fraudulent deductions and expenses on his customers' tax returns. He allegedly claimed fake mortgage interest deductions, illegally deducted Social Security taxes as state and local taxes, and fabricated employee business expenses, among other fraudulent items, on his customers' returns. According to the complaint, the harm to the United States from the preparer's misconduct could be \$7.8 million or more.

Source: <http://www.justice.gov/tax/2012/txdv12388.htm>

18. *March 28, Fort Worth Star-Telegram* – (Texas) **Ex-Bank of America branch manager pleads guilty to fraud.** A former Bank of America branch manager in River Oaks, Texas, accused of stealing more than \$2 million from customers' accounts over a 9-year period pleaded guilty March 28 in federal court to one count of bank fraud. She faces anywhere from probation to 30 years in prison and could be ordered to pay a \$1 million fine and restitution. Prosecutors allege the former manager used the money she stole for personal expenses, including vacations, clothing, jewelry, and land purchases. According to court documents, the woman was hired at the River Oaks branch in 1996, and was later promoted to personal banker, then assistant branch manager and finally branch bank manager. Her positions gave her full access to customers' bank accounts. Beginning around 2002 until April 2011, she withdrew cash from customers' bank accounts, sometimes forging signatures on withdrawal slips. She would inform tellers that she was withdrawing cash for the customer, sometimes lying by saying the customer was waiting inside her office. Prosecutors said she avoided having to fill out mandatory bank reports by never withdrawing more than \$10,000 per transaction. She targeted customers with whom she had had a longstanding relationship, knowing they would likely report any uncovered improper transactions directly to her. She would then refund their accounts with money stolen from other customers' accounts. Court documents state she prevented bank statements from being sent to customers' home by entering codes into the bank's data system indicating the customers' addresses were unknown.

Source: <http://www.star-telegram.com/2012/03/28/3842234/ex-bank-of-america-branch-manager.html>

19. *March 28, Portland Oregonian* – (Michigan; National) **Portland man ordered to pay back profits from fraudulent investment schemes.** A man has been ordered to return profits made from activities that resulted in a series of securities law violations, including his role in a Ponzi scheme that raised \$72.6 million from 3,000 investors, the Portland Oregonian reported March 28. A federal judge in Michigan ordered the man to repay investors \$4.1 million and to pay a \$100,000 civil fine. According to the U.S. Securities and Exchange Commission (SEC), the man had promoted himself on his

Web site, Mazu.com, as a trustworthy investment reviewer since 1997. He recommended some business opportunities, did not recommend others, and warned visitors how to spot and avoid a scam. Starting in 2006, the SEC alleged he promoted a series of fraudulent schemes, including the Ponzi scheme orchestrated by a Swartz Creek, Michigan man, who paid the defendant \$3.8 million for his participation. He promoted other schemes and guaranteed large returns, but had no basis for the claim, the SEC said.

Source:

http://www.oregonlive.com/business/index.ssf/2012/03/portland_man_ordered_to_pay_ba.html

20. ***March 27, Federal Bureau of Investigation – (National) FBI releases bank crime statistics for third quarter of 2011.*** During the third quarter of 2011, there were 1,094 reported violations of the Federal Bank Robbery and Incidental Crimes Statue, a decrease from the 1,325 reported violations in the same quarter of 2010, according to statistics released March 27 by the FBI. There were 1,081 robberies, 11 burglaries, 2 larcenies, and 1 extortion of a financial institution reported between July 1, 2011 and September 30, 2011. These statistics were recorded as of October 28, 2011.
Source: <http://www.fbi.gov/news/pressrel/press-releases/fbi-releases-bank-crime-statistics-for-third-quarter-of-2011>

[\[Return to top\]](#)

Transportation Sector

21. ***March 29, Associated Press – (Pennsylvania) Man detained at Philadelphia Airport.*** A Pennsylvania man was arrested and faces a federal charge after screeners found him trying to take powerful fireworks on a cross-country flight March 29. Authorities said the man had “commercial grade M-80s” in a backpack when passing through security at Philadelphia International Airport in Philadelphia as he was about to board a flight to San Francisco, a chief inspector said. He was stopped after screeners noticed an “anomaly” in the backpack, and never got through security. “He says that he has an interest in these items professionally,” the inspector said. The situation remained under investigation, but authorities said the explosives may have been left in a bag accidentally. The man is being charged with possession of a destructive device, and additional counts are likely. The checkpoint was closed for about 30 minutes, but no flights were delayed, an airport spokeswoman said.
Source:
http://online.wsj.com/article/SB10001424052702303816504577311401280906824.html?mod=googlenews_wsj
22. ***March 29, Associated Press – (Indiana) Residents allowed back home near site of northeastern Indiana freight train derailment, fire.*** Trains were running again on a busy northeastern Indiana line that was closed by a freight train derailment and fire. A Norfolk Southern spokesman said March 29 that the last of the burning cargo was extinguished overnight at the site of the derailment near Ligonier, about 40 miles northwest of Fort Wayne, Indiana. Cars carrying molten sulfur and wine bottles packed

in cardboard boxes caught fire after the March 27 derailment. Between 90 and 100 trains use the line each day, including two daily Amtrak passenger trains. Some residual delays could occur on the line March 29 because of backlogged shipments. Also, residents from a dozen or so homes near the the site of the derailment were allowed to return home early the afternoon of March 29.

Source:

<http://www.therepublic.com/view/story/314de2927a304419947ab7399deb9f94/IN--Indiana-Train-Derailment/>

23. ***March 28, CNN.com*** – (New York; Texas) **JetBlue pilot charged with interfering with flight crew.** A JetBlue pilot was charged with interfering with a flight crew after his midair behavioral meltdown led to an emergency landing. The federal criminal complaint revealed details of the March 27 incident on a flight from New York's John F. Kennedy International Airport en route to Las Vegas in which the pilot displayed what passengers and fellow crew members described as erratic, bizarre, and disturbing behavior. His behavior that included ranting and yelling and attempts to charge through the cockpit door and using a lavatory on the plane, forced a copilot to make an emergency landing in Amarillo, Texas. The pilot who had the meltdown has been suspended pending an investigation and was receiving medical treatment, the airline said March 28. If convicted, he would face a maximum 20 years in prison and a \$250,000 fine.

Source: http://www.cnn.com/2012/03/28/travel/jet-blue-flight-diverted/index.html?hpt=us_c2

24. ***March 26, Billings Gazette*** – (Montana) **Copper thieves targeting rail lines.** Thieves made at least seven raids in four weeks on copper wire strung along railroad tracks from Huntley to Laurel, Montana, the Billings Gazette reported March 26. “We see thievery whenever metal prices go up,” said a Yellowstone County Sheriff’s Department captain. “But this has been quite an increase this past month.” March 19, someone stole wire between Billings and Laurel along Montana Rail Link’s (MRL) right-of-way running parallel to Interstate 90. March 21, someone ran off with wire in the same area. These two thefts will cost MRL at least \$7,500, including the labor and wire to make the repairs. Burlington Northern Santa Fe was investigating copper theft across its system and is cracking down on trespassers because of the theft problem and accidents when people get too close to trains.

Source: http://billingsgazette.com/news/local/copper-thieves-targeting-rail-lines/article_be7a83ea-527b-51cb-9cf5-4fb97bec5e7b.html

For another story, see item [3](#)

[\[Return to top\]](#)

Postal and Shipping Sector

See item [14](#)

[\[Return to top\]](#)

Agriculture and Food Sector

25. ***March 29, Canadian Press*** – (International) **Inspectors find more cases of salmon virus at Nova Scotia fish farm.** The Canadian Food Inspection Agency said it could take months before a Nova Scotia fish farm at the center of a salmon virus outbreak is removed from quarantine, the Canadian Press reported March 29. The federal agency said on its Web site it confirmed additional cases of infectious salmon anemia at a commercial aquaculture operation in the province. It does not name the facility, but Cooke Aquaculture has said the virus was discovered at the firm's operation in Shelburne Harbour. Cooke first detected the virus during routine testing in February. The agency said the facility will remain under quarantine until all fish have been taken from the site and all pens, cages, and equipment have been disinfected. The virus poses no threat to human health or food safety, but it can kill up to 90 percent of the salmon it infects.
Source: <http://www.winnipegfreepress.com/arts-and-life/life/greenpage/inspectors-find-more-cases-of-salmon-virus-at-nova-scotia-fish-farm-144883155.html>
26. ***March 29, Associated Press*** – (International) **UN: Egypt's foot-and-mouth outbreak could spread.** A U.N. agency is warning that an outbreak of foot-and-mouth disease in Egypt could spread and threaten livestock in North Africa and the Middle East, leading to possible food shortages, the Associated Press reported March 29. The disease is not a direct threat to humans, but meat and milk from sick animals are unsafe for consumption. The Italy-based Food and Agriculture Organization said 40,222 cases of the disease are suspected in Egypt and 4,658 animals, mostly calves, have already died. The agency said 6.3 million buffalo and cattle and 7.5 million sheep and goats are at risk in Egypt. The agency said Egypt needs regional help in obtaining vaccines.
Source: <http://www.9news.com/news/article/259578/188/UN-Egypt's-foot-and-mouth-outbreak-could-spread>
27. ***March 28, Food Safety News*** – (Alabama) **Alabama McDonald's customers possibly exposed to hepatitis A.** Customers who ate at a McDonald's in Northport, Alabama, between February 28 and March 14 may have been exposed to hepatitis A through an infected employee, according to the Alabama Department of Health. In a news alert, state health officials advised customers who visited the McDonald's any time March 14 or during breakfast hours March 16 to contact a health care provider as soon as possible. "Hepatitis A vaccine and immune globulin can prevent hepatitis A virus infection, but only when given within 14 days of exposure," explained a state health officer. Therefore, individuals exposed March 14 or 16 should receive treatment no later than March 30. Signs and symptoms of hepatitis A virus infection appear 2 to 6 weeks after exposure. The disease varies in severity, from mild cases lasting 2 weeks or less to more severe cases lasting 4 to 6 weeks or longer.
Source: <http://www.foodsafetynews.com/2012/03/alabama-mcdonalds-customers-possibly-exposed-to-hepatitis-a/>
28. ***March 27, Holyoke Enterprise*** – (Colorado) **Anhydrous ammonia leak injures Grainland Cooperative employee.** The Grainland Cooperative agronomy plant manager was seriously injured following a hazardous material accident March 22

northeast of Holyoke, Colorado, the Holyoke Enterprise reported March 27. The Holyoke Volunteer Fire Department was called to an anhydrous ammonia leak at Grainland's east facility. The plant manager and another employee were changing a pump on a line when a leaky valve began to spray anhydrous ammonia. The plant manager, who was closer to the leak, received burns on his legs. Once a tank is leaking, there is no shutting it down, the Grainland CEO said. Firefighters spent nearly 5 hours in rainy conditions applying water to the leak and searching for valves to shut the system down. A HAZMAT unit with the Colorado State Patrol responded. Two Holyoke firefighters were taken to the hospital for ammonia exposure. Both were treated and released, the fire chief said. Area homes and businesses were warned about the leak but no mandatory evacuations were ordered.

Source:

http://www.holyokeenterprise.com/index.php?option=com_content&view=article&id=5092:anhydrous-ammonia-leak-injures-grainland-cooperative-employee&catid=34:local-news&Itemid=34

29. ***March 26, US Food Safety*** – (National) **Kroger Private Selection Fresh Salsa and pico de gallo recalls.** The Kroger Co. is recalling its Private Selection Fresh Salsa and Private Selection Pico de Gallo because the products may be contaminated with Salmonella and if eaten, could result in severe illness, US Food Safety reported March 26. The products affected by this recall are Private Selection Fresh Salsa; Private Selection Salsa, hot; and Private Selection Pico de Gallo. Affected Kroger stores are located in the following states: Ohio, Kentucky, Indiana, West Virginia, Tennessee, Arkansas, Mississippi, North Carolina, and Virginia. Jay C, Food4Less, and FoodsCo stores are affected as well.

Source: <http://www.usfoodsafety.com/zr120051.aspx>

30. ***March 24, Sacramento Bee*** – (California) **SK Foods' former CEO pleads guilty, faces up to 7 years in prison.** After more than 6 years of investigation, poring over more than 1 million documents and wiretaps, and the guilty pleas of 10 midlevel food-industry executives, the federal government got a guilty plea from the former owner and chief executive officer of SK Foods LP in Monterey, California. The man pleaded guilty to racketeering and price-fixing in a deal favorable to him that calls for no more than 7 years in prison. The man, whose firm provided tomato products that ended up in most of the homes in this country, had faced up to 20 years in prison if convicted at trial of plotting widespread bribery as part of a conspiracy to gain the upper hand on his competitors. He was said to have provided more than \$100,000 in bribes to purchasing agents at firms such as Frito-Lay, Kraft Foods, Safeway, and ConAgra to win sales contracts, and to have falsified records that enabled the sale of old and moldy tomato products that found their way into the American food chain. The man also must turn over his interest in \$3.25 million in an Andorra bank account he opened after learning he was under investigation.

Source: http://www.modbee.com/2012/03/24/2127108/sk-foods-former-ceo-pleads-guilty.html#storylink=omni_popular

For more stories, see items [5](#) and [32](#)

[[Return to top](#)]

Water Sector

31. ***March 28, Wooster Daily Record*** – (Ohio) **Settlement reached with Ohio EPA.** The city of Wooster and the Ohio Environmental Protection Agency (OEPA) reached a settlement regarding an enforcement action taken against the city for multiple years of violations against the Clean Water Act at the wastewater treatment plant, the Wooster Daily Record reported March 28. As part of the settlement, the city agreed to a \$10,000 penalty to the OEPA. Wooster will also modify its operations pending an OEPA review of a comprehensive study of the Wooster wastewater plant. A study of the Killbuck Creek Watershed said the city had a history of exceeded permitted effluent limits in its National Pollutant Discharge Elimination System permit. The settlement document states the city was in significant noncompliance from the second quarter of 2006 to the second quarter of 2011. It additionally states the city's inability to maintain compliance is due to "high flow events in portions of its collection system as well as high strength wastewater from industrial users."

Source: <http://www.the-daily-record.com/news/article/5172599>

32. ***March 28, Associated Press*** – (Maryland) **Sewage leak closes shellfishing near Baltimore.** Maryland environmental officials have warned the public to avoid waters of the Chesapeake Bay and the Patapsco River after a 54-inch main broke March 25 at a Baltimore County pumping station. Sewage has continued to leak since the break, but Maryland Department of the Environment officials said crews were expected to begin pumping the area around the break March 28. Shellfish harvesting has been closed at the mouth of the Patapsco and nearby portions of the bay.

Source: <http://baltimore.cbslocal.com/2012/03/28/sewage-leak-closes-shellfishing-near-baltimore/>

33. ***March 28, KOVR 13 Sacramento*** – (California) **Two rescued from pump house near Sac State.** A man and a woman who broke into a pump house on the American River near the Sacramento State campus in Sacramento, California, were rescued by fire personnel March 27 and the man was arrested. Sacramento firefighters were dispatched to the pump house after two people became trapped inside after scaling several fences to access the five-story building connected to the Fairbairn Water Treatment Plant. The woman apparently fell into a suction pool inside the pump house and the man was unable to get her out. The woman was taken to a hospital after suffering from hypothermia, and a warrant request for trespassing was submitted for her arrest, according to police. Fire officials said the two appeared to be intoxicated. The water treatment plant has had several security upgrades because water treatment facilities were classified as potential terrorist targets after the September 11th attacks. Firefighters said they walked in through an unlocked gate, but city officials would not say how they got inside and did not comment on security at the facility.

Source: <http://sacramento.cbslocal.com/2012/03/28/breaking-two-trapped-in-pump-house-near-sac-state/>

34. *March 27, Associated Press* – (Washington; International) **Wash. officials track Columbia River sewage spills.** The Washington state Department of Ecology is tracking two sewage spills into the Columbia River. The British Columbia environment ministry said that a sewage pipe leak was repaired March 27 in Trail, British Columbia, and sewage was flowing normally to a wastewater treatment plant. Trail is about 10 miles north of the U.S.-Canada border. Ecology said the estimate of that sewage spill was reduced to about 1.15 million gallons. The ecology department was also working with East Wenatchee, Washington officials to determine the cause of a 500,000-gallon sewage spill into the river March 25. The plant has since returned to normal operations. Source: <http://www.seattlepi.com/news/article/Wash-officials-track-Columbia-River-sewage-spills-3438482.php>

For more stories, see items [4](#), [51](#), and [53](#)

[\[Return to top\]](#)

Public Health and Healthcare Sector

35. *March 27, ABC News* – (Washington) **Washington state hit hard by whooping cough.** Whooping cough is hitting the State of Washington particularly hard, ABC News reported March 28. Numbers released March 27 showed that whooping cough cases have risen to 549 in 2012. At this time in 2011, there were 88 pertussis cases in the state, said the communications director of Washington's health department. The annual number of cases will likely exceed the 950 yearly total the state saw in 2011. Source: <http://abcnews.go.com/blogs/health/2012/03/28/washington-state-hit-hard-by-whooping-cough/>

For more stories, see items [6](#), [27](#), [51](#), and [53](#)

[\[Return to top\]](#)

Government Facilities Sector

36. *March 29, Ardmore Daily Ardmoreite* – (Oklahoma) **Madill Elementary School evacuated.** Students were out of school district-wide March 29 following the evacuation of Madill Elementary in Madill, Oklahoma, March 28. The evacuation occurred March 28, after three students and a teacher reported symptoms of dizziness and nausea. Emergency personnel were contacted, with officials suspecting a gas leak. A total of 25 people were transported from the school to area hospitals. As of March 28, no traces of gas leaks, carbon monoxide, or other contaminants had been found. School officials cancelled school and activities scheduled for March 29 to thoroughly sanitize all district buildings. The process included disinfecting desks, restrooms, and chairs. The regional health department and other emergency personnel will check the schools March 29 before they are reopened. School officials expected to be back in class March 30.

Source: <http://www.ardmoreite.com/news/x221021383/Madill-Elementary-School-evacuated>

37. *March 28, CNN* – (Michigan) **Michigan militia members acquitted of conspiracy; leader faces lesser charges.** The trial against members of the so-called Hutaree militia resumed March 29 for the Michigan-based group’s leader and his son, who face weapons charges. The stakes, however, are considerably lower after a federal judge in Detroit March 27 dropped the more serious charges of sedition and conspiracy to use weapons of mass destruction against the government. The directed verdict cleared several of the original nine defendants of all charges. Federal authorities accused the nine members of the “Christian warrior” militia of homegrown terrorism. The FBI planted a secret informant and FBI agent in the militia in 2008 to record the activities of the group. The video and audio recordings became the crux of the federal case, including clips of the man’s son making anti-government statements and remarks about killing police officers. The defendants all faced a maximum sentence of life in prison. However, in a trial that began in February, the federal district judge said she did not find the government’s evidence sufficiently proved that the Hutaree militia had planned a conspiracy against the government. The remaining charges of weapons possession rest on the leader and his son, both of whom have already spent 2 years in prison. The government claims the two were in possession of unregistered automatic weapons. If convicted, the pair could face a maximum penalty of 10 years in prison.

Source: http://www.cnn.com/2012/03/28/justice/michigan-militia-trial/index.html?hpt=us_c2

For more stories, see items [6](#), [10](#), [11](#), [39](#), and [43](#)

[[Return to top](#)]

Emergency Services Sector

38. *March 29, WOWK 13 Huntington* – (Ohio) **Scioto County 911 service partially available.** Officials in Scioto County, Ohio, said their regular 911 service is unavailable, but dialing 911 itself is now functioning, after experiencing a system-wide outage, WOWK 13 Huntington reported March 29. Instead of routing to the county call center, 911 will route to the Scioto County sheriff’s non-emergency line. Officials with Frontier Communications were working to restore the full system. Previously, those with land line or cell service within the county were not able to dial 911 in case of an emergency.

Source: <http://www.wowktv.com/story/17281735/scioto-county-911-service-partially-available>

39. *March 29, Barrow Journal* – (Georgia) **County’s fire radio goes down along with Winder police, fire and city hall phones.** A contractor digging a ditch for a sewer line behind Winder, Georgia’s public safety buildings accidentally severed an underground utility line, totally disabling for hours the county’s fire radio base station located at the city fire department, along with the phone system for the Winder Fire Department, the Winder Police Department and Winder City Hall, a city administrator told the Barrow Journal March 28. City public works crews and utility company personnel restored the phone service in about 2 hours, the fire base station was brought back into operation in 3 hours.

Source: <http://www.barrowjournal.com/archives/6569-Countys-fire-radio-goes-down-along-with-Winder-police,-fire-and-city-hall-phones.html>

For more stories, see items [37](#) and [52](#)

[[Return to top](#)]

Information Technology Sector

40. *March 29, H Security* – (International) **Chrome 18 improves graphics performance, closes security holes.** Google released version 18 of Chrome. The new Stable channel release, labelled 18.0.1025.142, closes nine security holes, of which three are rated as “High severity.” These include high-risk use-after-free errors in SVG clipping, an off-by-one problem in OpenType Sanitizer, and memory corruption bugs in Skia. Other closed holes include five medium-severity problems such as out-of-bounds reads in SVG text and text fragment handling, a cross-site scripting bug, a SPDY proxy certificate checking error, and an invalid read in the V8 JavaScript engine. A low-severity bug used by the hacker “Pinkie Pie” during the Pwn2Own competition at CanSecWest was also closed. A Google employee said some of the fixes “represent the start of hardening measures based on study of the exploits submitted to the Pwnium competition.”

Source: <http://www.h-online.com/security/news/item/Chrome-18-improves-graphics-performance-closes-security-holes-1486421.html>

41. *March 29, The Register* – (International) **Kelihos zombies erupt from mass graves after botnet massacre.** Security researchers warned that the resurrected Kelihos botnet taken down March 28 is still active. Experts not involved in the operation said the miscreants behind the network of compromised Windows computers are working on their comeback. The zombie PC army was taken offline in September 2011, they said, yet later resurfaced. Seculert reports Kelihos-B, which was distributed as a Facebook worm over recent weeks, is still active and spreading — even after the shutdown attempt by CrowdStrike and Kaspersky Labs March 28. Seculert views this botnet as the undead remnants of Kelihos-B rather than the spawn of a new variant of the malware. The findings suggest sink-holing 109,000 backdoored machines infected with the spam-spewing and credential-stealing Kelihos trojan may not have disabled the entire bot network.

Source: http://www.theregister.co.uk/2012/03/29/kelhios_bot_not_dead_yet/

42. *March 28, eWeek* – (International) **iPhone passcodes can be cracked as quickly as XRY.** The four-digit password on Apple’s iPhone is no match for Micro Systemation’s XRY application, according to experts. The password on the popular smartphone can probably keep a regular person who finds the device from breaking into it. However, the software from the Swedish company, which it sells to law enforcement agencies, can crack the code on an iPhone or a smartphone running Google’s Android mobile operating system within minutes. XRY essentially jailbreaks the device in the same manner that regular jailbreakers do. It then runs every combination of four-digit passcodes until it hits the right one. Once that happens, all the data on the phone can be

accessed, according to the company.

Source: <http://www.eweek.com/c/a/Security/iPhone-Passcodes-Can-Be-Cracked-as-Quickly-as-XRY-708506/>

43. *March 28, SecurityWeek* – (International) **Attackers using Taidoor trojan to target think tanks and US-Taiwan interests.** In 2008, the Taidoor trojan made its first appearance on the Web. It started by attacking government agencies, but the group behind it expanded their reach by targeting a wide range of victims. Now, based on research from Symantec, it appears the group running Taidoor is interested in think tanks, especially those focused on Taiwan. While Taidoor started out by targeting governments, between 2009 and 2010, the malware shifted gears. Government victims were counted among those in the media, financial, telecom, and manufacturing sectors. The length of the attack, almost 4 years now, shows the group responsible for Taidoor is persistent if nothing else. Based on the collected data, Symantec said that since May 2011, there has been a substantial increase in activity. The malware's current targets are primarily private industry and international think tanks with a direct involvement in United States and Taiwanese affairs. Facilities in the services sector these organizations may use are also targeted.

Source: <http://www.securityweek.com/attackers-using-taidoor-trojan-target-think-tanks-and-us-taiwan-interests>

44. *March 28, Dark Reading* – (International) **Cybercriminals' love affair with Havij spells SQL injection trouble.** Today's exponential increase in attack volume and complexity can largely be attributed to cybercriminal working smarter with powerful, automated tools. In the database-cracking world, Havij stands as one of the most popular of these tools: and as such, it should be on the radar of any security professional seeking to prevent costly data breaches within their environments. "If you're talking about databases and the tools that are used to perform SQL injection, Havij is one of the most common," a senior security strategist at Imperva said. Havij was developed by Iranian hackers in the spring of 2010. The tool has so captured the hearts and minds of the black hat community, that groups like Anonymous frequently train on how to wreak havoc using it, said the chief technology officer at Application Security, Inc. Favored by hacktivists and financially motivated attackers, Havij automates criminals' SQL injection attacks by automatically detecting the database behind a targeted Web site, detecting whether it uses a string or integer parameter type, and testing different injection syntaxes. Unlike a lot of penetration tools, Havij can not only point to potential vulnerabilities, it can also carry out data extraction and harvesting.

Source: <http://www.darkreading.com/database-security/167901020/security/news/232700449/cybercriminals-love-affair-with-havij-spells-sql-injection-trouble.html>

45. *March 28, Computerworld* – (International) **Duqu malware resurfaces after four-month holiday.** Duqu is back, security researchers said March 28. After a several-month sabbatical, the Duqu makers recompiled one of the trojan's components in late February, said the manager of operations at Symantec's security response team. The system driver, which is installed by the malware's dropper agent, is responsible for

decrypting the rest of the already-downloaded package, then loading those pieces into the PC's memory. Symantec captured a single sample of the driver, which was compiled February 23, 2012. Before that, the last time the Duqu gang updated the driver was October 17, 2011. Duqu has been characterized by Symantec and others as a possible precursor to the next Stuxnet, the ultra-sophisticated worm that sabotaged Iran's nuclear fuel enrichment program by crippling critical gas centrifuges. The Symantec manager said the functionality of the new driver was "more or less the same" as earlier versions, including the one spotted October 2011 and another from late 2010 that later surfaced. March 27, the leader of Kaspersky's global research and analysis team said the Duqu driver was probably modified to evade security software and Duqu detection programs.

Source:

[http://www.computerworld.com/s/article/9225637/Duqu_malware_resurfaces_after_for_month_holiday?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+\(Computerworld+Security+News\)&utm_content=Google+Rea](http://www.computerworld.com/s/article/9225637/Duqu_malware_resurfaces_after_for_month_holiday?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_content=Google+Rea)

46. ***March 27, U.S. Federal Trade Commission – (International) FTC charges that security flaws in RockYou game site exposed 32 million email addresses and passwords.*** The operator of a social game site agreed to settle charges that, while touting its security features, it failed to protect the privacy of its users, allowing hackers to access the personal information of 32 million users. The Federal Trade Commission (FTC) also alleged in its complaint against RockYou that the company violated the Children's Online Privacy Protection Act Rule (COPPA Rule) in collecting information from about 179,000 children. The proposed FTC settlement order with the company bars future deceptive claims by the company regarding privacy and data security, requires it to implement and maintain a data security program, bars future violations of the COPPA Rule, and requires it to pay a \$250,000 civil penalty to settle the COPPA charges.

Source: <http://ftc.gov/opa/2012/03/rockyou.shtm>

For more stories, see items [10](#), [47](#), and [48](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <https://www.it-isac.org>

[[Return to top](#)]

Communications Sector

47. ***March 28, CSO – (International) Operation Global Blackout: Real danger or irrelevant?*** Will the hacker group Anonymous make good on its threat to take down the Internet March 31? Probably not. But it could slow it down, according to many

security experts. It may depend in part on how unified Anonymous is about the attack. Anonymous threatened retaliation for the arrests of about 25 of its members in February, and is also focused on what its members believe is a continuing threat by Congress to censor the Internet through anti-piracy legislation. Anonymous is daring anyone to stop Operation Global Blackout — the group announced March 31 as the date of the attack, along with the method they intend to use — disabling the Domain Name Service (DNS) through distributed denial of service attacks on the root servers of the DNS with a tool called “ramp,” or “reflective amplification.” Even with the advance warning, a professor in the department of computing at the University of Surrey believes Anonymous could do some damage. In a piece for BBC, he said the top-level DNS systems are in different countries, are monitored by different organizations, and run on different technologies. He said Anonymous could bring a server down with ramp, in which an army of bots spoof the IP address of a target system and, “cause the DNS to flood the very network it is supposed to be serving.”

Source:

[http://www.computerworld.com/s/article/9225635/Operation_Global_Blackout_Real_danger_or_irrelevant/?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+\(Computerworld+Security+News\)&utm_content=Google](http://www.computerworld.com/s/article/9225635/Operation_Global_Blackout_Real_danger_or_irrelevant/?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_content=Google)

48. *March 28, Biloxi Sun Herald* – (Mississippi) **Cut cable silences C Spire phone service.** C Spire Wireless customers in south Mississippi lost service March 29 when a fiber-optic cable was cut. A C Spire Wireless spokesman said an independent third party was found to have cut an underground cable, between Seminary and Hattiesburg, resulting in a service outage sometime before noon. Shortly before 4 p.m., he said service had been restored to virtually 100 percent of customers. He could not estimate how many customers lost service. “The primary impact was voice service, although we have gotten some scattered reports from some customers (saying) that they also couldn’t text,” he said.

Source: <http://www.sunherald.com/2012/03/28/3849175/cut-cable-silences-c-spire-phone.html>

For more stories, see items [42](#) and [46](#)

[[Return to top](#)]

Commercial Facilities Sector

49. *March 29, Kalamazoo Gazette* – (Michigan) **Apartments evacuated when meth lab explodes in Sturgis Township complex.** One man was arrested and police were searching for another man they believe was involved in a March 28 explosion of a methamphetamine lab in an apartment in Sturgis Township, Michigan. According to a news release from the St. Joseph County Sheriff’s Office, deputies evacuated the other apartments in the complex while the St. Joseph County Area Narcotics Unit responded and removed the meth lab and waste. One man was arrested later that night at his home. Another man was at large and has warrants for his arrest for an unrelated incident.

Source:

http://www.mlive.com/news/kalamazoo/index.ssf/2012/03/apartments_evacuated_when_meth.html

50. *March 29, Tacoma News Tribune* – (Washington) **Workers say fire on Tacoma Tideflats started in paint can.** A fire that threw up plumes of smoke and leveled a small office building March 28 in Tacoma, Washington, might have been caused by a can of paint that caught fire, spreading flames to adjacent areas. The blaze drew a dozen fire vehicles and nearly three dozen firefighters who extinguished flames that destroyed the office building and damaged an attached, two-story wooden warehouse. No one was injured in the fire, which caused about \$190,000 in damage. The cause of the fire still was under investigation. Some workers at the site said a can of paint had caught fire and ignited areas of the wooden structure.
Source: <http://www.thenewstribune.com/2012/03/29/2086772/workers-say-fire-started-in-paint.html>

51. *March 29, Associated Press* – (Minnesota) **Another Minn. water park linked to cryptosporidium.** Another water park in Minnesota was linked to the intestinal disease cryptosporidiosis, the Associated Press reported March 29. Minnesota Department of Health officials said a case of the water-borne disease was connected to the Lodge at Brainerd Lakes. A state epidemiologist said the lodge worked with the department's environmental health officials and highly chlorinated the water park. The pool was closed March 26 and reopened March 29. The Brainerd Dispatch said the health department confirmed one case of the disease linked to the lodge's water park and at least two other suspected cases. The health department recently linked the parasitic disease to the Edgewater Resort and Water Park in Duluth.
Source: <http://www.kare11.com/news/article/970160/396/Another-Minn-water-park-linked-to-cryptosporidium>

52. *March 28, WCBS 2 New York* – (New York) **Six people injured in 3 alarm lower East Side apartment fire.** Six people suffered minor injuries in a three-alarm fire that raged for more than an hour in New York City, March 28. The fire started on the 16th floor of a 20-story high-rise, and quickly spread to the 15th and 17th floors. More than 100 firefighters responded to the scene. Four firefighters and two civilians were treated at a hospital for smoke inhalation. The cause of the fire was under investigation.
Source: <http://newyork.cbslocal.com/2012/03/28/three-alarm-fire-rages-on-lower-east-side/>

53. *March 28, Duluth News Tribune* – (Minnesota; Wisconsin) **Waterborne disease outbreak is traced to Duluth water park.** An outbreak of a waterborne diarrheal disease has been linked with Duluth's Edgewater Resort and Water Park, a Minnesota health official said March 27. Three cases of cryptosporidiosis have been confirmed, and six more are suspected in Minnesota and Wisconsin, said an epidemiologist for the Minnesota Department of Health who specializes in the disease. The cases involved adults and children, and all of those who came down with the illness spent time at the water park during March 2012. The epidemiologist said many other cases may have gone unreported. The water park voluntarily closed March 26, and all of the water facilities were treated with super-chlorination to kill the parasite. The water park

reopened March 27. The parasite is spread through the feces of infected humans, according to the Wisconsin Division of Public Health. Cryptosporidiosis is one of the most frequent causes of waterborne illness in the United States, according to the Centers for Disease Control and Prevention.

Source: <http://www.duluthnewstribune.com/event/article/id/226895/group/homepage/>

For more stories, see items [6](#) and [43](#)

[\[Return to top\]](#)

National Monuments and Icons Sector

54. *March 29, WSAZ 3 Charleston* – (West Virginia) **Brush fire burns nearly 250 acres.** A large brush fire burned nearly 250 acres in Nicholas County, West Virginia, according to a March 29 news release from the Nicholas County Division of Homeland Security and Emergency Management. Forestry officials believed the fire was under control as of March 29. The West Virginia Division of Forestry, Summersville Fire Department, Birch River Fire Department, Craigsville Fire Department, Nettie Fire Department, and Nicholas County Homeland Security and Emergency Management crews responded and spent more than 12 hours getting the fire under control. The cause of the fire was under investigation.

Source:

http://www.wsaz.com/news/headlines/Brush_Fire_Burns_Nearly_250_Acres_144740275.html

55. *March 29, Fox News* – (Colorado) **Colorado crews contain 15 percent of deadly fire that claimed 4,100 acres.** Crews made progress on a wildfire that killed two people in the mountains southwest of Denver and scorched 4,100 acres, Fox News reported March 29. Jefferson County, Colorado officials said the fire was 15 percent contained as firefighters were aided by a second straight day of favorable weather. Lighter winds allowed fire managers to think about helping the 900 residents forced to evacuate their homes. They have been out since a wind-swept fire raced through the canyons of the Rocky Mountain foothills March 26. It was confirmed that a prescribed burn conducted by the Colorado State Forest Service was to blame. An investigation was launched into what went wrong. Fire officials said safety precautions were taken as a perimeter was established around the 50-acre controlled burn site. On the fourth day of mop-up, 70 mph winds blew a hot spot past the containment. Colorado's governor banned prescribed burns as the disaster is investigated. Two people were killed in the fire and a woman whose house was destroyed is still listed as missing. More than 400 firefighters continue to battle the fire. The National Guard was activated and there was a full air assault being conducted with two air tankers, other fixed wings planes, and four helicopters. There was some urgency to get the fire under full control as soon as possible, as strong winds were forecast for March 31.

Source: <http://www.foxnews.com/us/2012/03/29/colorado-crews-contain-15-percent-deadly-fire-that-claimed-4100-acres/?test=latestnews>

56. *March 28, Rapid City Journal* – (South Dakota) **Fire burning southeast of Custer.** The Apple Fire in the Black Hills National Forest in South Dakota was estimated at 200 acres as of March 28, according to a fire information officer. The fire was caused by lightning. Forest Service, state, and volunteer firefighters were on the scene southeast of Custer. A single engine aircraft and a National Guard Black Hawk helicopter were called in to assist with the fire.
Source: http://rapidcityjournal.com/news/fire-burning-southwest-of-custer/article_1ab500e0-7911-11e1-921c-001a4bcf887a.html

[[Return to top](#)]

Dams Sector

Nothing to report

[[Return to top](#)]



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: <http://www.dhs.gov/IDailyReport>

Contact Information

Content and Suggestions:

Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2267

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.